Last Updated: Tuesday, April 14, 2009

PCI: An Industry Standard for Protecting Consumer Credit Cards on the Internet

By
James M. Dzierzanowski, Ph.D.

Identity theft and credit card fraud are the fastest growing crimes in the United States. The Federal Trade Commission reports that one in six Americans will be a victim of identity theft this year and that identity theft has been the No. 1 consumer complaint for the last four years. More than 100 million personally-identifiable, customer records have been breached in the US over the past two years, most of these breaches occurred at companies that are household names[1].

Banks and credit card companies are responding quickly and aggressively to the challenge, fearing a potential backlash of consumers discouraged from using credit cards based on security concerns. In 2004, many companies banded together to form the Payment Card Industry (PCI) Security Standards Council, and developed standards and policies that must be met by all vendors who accept credit card transactions. The council members include American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa International; they collaborated to create an industry-wide, global framework that details how companies handle credit card data – specifically, banks, merchants and payment processors. The result was the Payment Card Industry (PCI) Data Security Standard (DSS)[2], a set of best practice requirements for protecting credit card data throughout the information lifecycle. The PCI compliance security standards are technical and operational requirements that were created to help organizations that process credit card payments prevent credit card fraud, hacking and various other security vulnerabilities and threats.

[1] Source: www.privacyrights.org
[2] Source: www.pcisecuritystandards.org

Very simply, the PCI DSS requirements are applicable if a Primary Account Number (credit card number) is stored, processed, or transmitted. These security requirements apply to all system components. The PCI standard itself centers on six high-level control objectives – essentially, targets for security that bolster the protection of the credit card information. Broad security requirements support each control objective, and these twelve requirements are further dissected through well over 200 sub-requirements that specify the technologies, policies and procedures necessary for protecting cardholder data.

The major credit card companies require compliance with PCI DSS rules via contracts with merchants and their vendors that accept and process credit cards. If a member, merchant, or service provider does not comply with the security requirements or fails to rectify a security issue, they may face fines up to US$500,000 per incident[3] or restrictions imposed by the credit card companies, including denying their ability to accept or process credit card transactions.

Banks, merchants and payment processors must approach PCI DSS compliance as an ongoing effort. Compliance must be validated annually, and companies must be prepared to address new aspects of the standard as it evolves based on emerging technologies and threats.

Companies in recent years have invested substantial time and money in achieving and validating compliance with PCI data Security Standards (DSS). Recently, Visa has reported that most of the nation's largest retailers are now compliant with the industry.

[3] Source: www.verisign.com

Understanding PCI DSS Security Requirements

The PCI DSS requirements encompass 12 requirements and are organized in 6 logically related groups, which are "control objectives."

Control Objectives	Requirements
Build and maintain a secure network	1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect cardholder data	3. Protect stored cardholder data (Render the Primary Account Number, at minimum, unreadable anywhere it is stored) 4. Encrypt transmission of cardholder (Use strong cryptographic and security protocols to safeguard sensitive cardholder data during transmission) data across open, public networks
Maintain a vulnerability management program	5. Use and regularly update anti-virus software 6. Develop and maintain secure systems and applications (Develop all web applications based on secure coding guidelines)
Implement strong access control measures	7. Restrict access to cardholder data by business need-to-know 8. Assign a unique ID to each person with computer access (Render all

	passwords unreadable during transmission and storage on all system components) 9. Restrict physical access to cardholder data (Maintain strict control over the internal and external distribution of any kind of media that contains cardholder data, including destruction of media)
Regularly monitor and test networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an information security policy	12. Maintain a policy that addresses information security

PCI Assessment Failings:

A large and reputable security firm reviewed samples of their assessments and found that companies, even with strong security programs in place, failed to pass due to the following (in order of frequency):

1. Not protecting stored data (Requirement 3)
2. Not, regularly test security systems and processes (Requirement 11)
3. Did not, assign a unique ID to each person with computer access, i.e. passwords (Requirement 8)
4. Did not, track and monitor all access to network resources and cardholder data (Requirement 10)
5. Did not, install and maintain a firewall to protect data (Requirement 1)
6. Did use vendor-supplied defaults for system passwords and other security parameters (Requirement 2)

Other Common Findings Derived from PCI Compliance Failure:

- Merchants typically keep too much data, organizations typically store much more about the credit card than just the card numbers. Organizations processing a high volume of transactions exhibit the most egregious behavior, however a counter point is merchant claims for fraud reduction.
- Encryption and access control are the top challenges.
- Organizations are using PCI compliance as an opportunity to increase security, mitigating the risk of data breaches is the top driver for PCI compliance. ISO 17799 and 27001 remain the predominate frameworks being used to comply with PCI.
- Point of Sale (POS) application vulnerabilities. Applications may be creating logs that store card track data. While PCI requirements prohibit the storage of track data under any circumstances, nefarious individuals may subvert applications that typically store this data.

In addition to PCI non-compliance findings, a key data point for understanding security challenges in credit-card processing environments are derived from the actual compromises that occur in the field, they include:

- **Unsecured physical assets.** Unencrypted data may be stored on backup tapes and other mediums that are prone to loss or the left.
- **Unencrypted spreadsheet data.** Users may be storing card data in spreadsheets, flat files, or other formats that are difficult to control as they are transferred top laptops, desktops, and wireless devices.
- **Poor identity management.** Users and administrators may not be handling authentication properly. Passwords can be easily shared, stolen, or guessed.
- **Network architecture flaws; flat networks.** Many businesses did not develop their IT infrastructure with security in mind. Networks are very flat (non-partitioned) in which card databases are not segmented from the rest of the network.

- **Lack of log monitoring and intrusion detection system (IDS) data;** poor logging tools. Insufficient data makes it more difficult to investigate compromises.
- **Card numbers in the DMZ.** POS terminals may be storing credit card numbers in the externally facing perimeter network. Frequently, these systems are also storing track data.

Recent Enhancements to the PCI Security Standard:

Recent focus includes heightened security requirements for wireless networks due to the jump in the use of wireless POS terminals. The PCI council has updated the security standards to include wireless IEEE 802.11i, which strongly authenticates and encrypts the transmission of cardholder data, ceasing use of WEP (Wired Equivalent Protocol), effective March 31, 2009 an algorithm to secure wireless networks. Security experts generally consider WEP to be a less secure method for protecting wireless data than other methods. In addition to wireless improvements, the council now requires the protection of public-facing web applications by either (1) reviewing or patching vulnerabilities, or (2) installing web-application firewalls. Followed by addressing web application security, the council suggests critical review of employee-facing technologies, such as remote access, removable electronic media, email usage, laptops and personal digital assistants. Lastly, the council strongly suggests regular penetration testing done either internally or my third party, to examine possible vulnerabilities by simulating an attack.

Benefits:

- Know here all your organization's credit card data resides, in order to take steps to ensure that information is secure
- Protect card data wherever it resides across the organization, prove the identities of individuals accessing it and ensure that only those with a true business need have rights to access the data
- Monitor and track access to cardholder data, so when a policy or security violation occurs, you will know and be able to respond

- Understand how the investments you've made in addressing PCI can be leveraged beyond the audit, to help improve data security and protect the business across the enterprise

Lastly, it is often surprising to see how many compromises and PCI audit failures could be avoided by improving security awareness. Continually educate and train internal staff; develop processes that ensure adherence to security procedures and policies.

PCI is not unlike any good security program, where understanding risks, sound design and implementation, coupled with operational excellence; all combine to deliver sound and secure business solutions.

For more information:

http://usa.visa.com